Регламент

Организация работы

Редакция 2.0

утверждено приказом №011 от 15.04.2019г.

Содержание

	Раздел	Страница
	Глава 1. Термины и определения	3
	Глава 2. Описание системы	4-6
	Глава 3. Управление	7-9
	Глава 4. Информационная безопасность	10-19

Глава 1. Термины и определения

1. Общие термины и определения

1.1. Все неуказанные термины и определения применяются из нормативных актов и законодательства.
1.2. Данные – любая информация в любой форме, в том числе как запись в базе данных, файл, сообщение.
1.3. Обработка данных - сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменения), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение данных.
1.4. Безопасность данных - исключение несанкционированного доступа к данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение данных.
1.5. Угроза безопасности данных – совокупность условий, создающих опасность несанкционированного доступа к данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение данных, а так же иные неправомерные действия.
1.6. Персональные данные – информация, касающаяся конкретного физического лица, которая включает в себя факты, события и обстоятельства жизни гражданина, позволяющие идентифицировать его личность.
1.7. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
1.8. Аутентификация – присвоение субъектам и объектам доступа пароля или биометрических данных или их сравнение.
1.9. Контролируемая зона – пространство (здание, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
1.10. Инцидент - происшествие, связанное со сбоем в функционировании системы, вызываемое в результате непреднамеренных и преднамеренных действий пользователей и третьих лиц или возникновения обстоятельств непреодолимой силы.
1.11. Уязвимость – слабость в системе защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
1.12. Недекларированные возможности – функциональные возможности программного обеспечения, не описанные в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности данных.

2. Термины и определения для регламента

2.1. Провайдер – компания, предоставляющая доступ к системе.
2.2. Клиент – компания получающая доступ к системе. Клиент может состоять из нескольких компаний (юридических лиц или индивидуальных предпринимателей), объединяемых в группу компаний.
2.3. Система – информационная система, состоящая из программ, данных, оборудования, информационных технологий, предоставляемых Клиенту.
2.4. Сотрудники – сотрудники Провайдера и сотрудники Клиента.

Глава 2. Описание системы

1. Общие положения

1.1. Система предоставляется как сервис и является клиент-серверной системой с доступом с помощью браузера.
1.2. Система является медицинским изделием, должна быть зарегистрирована в соответствии действующим с законодательством и иметь регистрационное удостоверение.
1.3. Система является «программой ЭВМ» и должна быть зарегистрирована в соответствии с действующим законодательством.

2. Сервисы системы

2.1. Система предоставляет следующие основные сервисы:
2.1.1. Numedy.MIS (Medical Information System) – медицинская информационная система, обеспечивает управление медицинской организацией, ведение справочников, документооборота, работу с медицинскими протоколами, заключениями и измерениями, формирование отчетов, управление рабочими потоками, графиками работ и загрузки, связью и контактами, настройками.
2.1.2. Numedy.Viewer – обеспечивает просмотр, редактирование и реконструкцию изображений различных форматов, просмотр видео, построение графиков.
2.1.3. Numedy.DeviceManager – обеспечивает взаимодействие системы и различного оборудования, управление оборудованием, передачу и получение данных и файлов в различных форматах.
2.1.4. Numedy.PACS – обеспечивает взаимодействие системы и оборудования по протоколу DICOM, управление оборудованием, передачу и получение данных и файлов в формате DICOM.
2.1.5. Numedy.Conference – обеспечивает работу видеоконференций.
2.1.6. Numedy.Exchange – обеспечивает обмен данными с различными внешними сервисами, в том числе с государственными органами.
2.1.7. Numedy.AtlasPatient – личный кабинет пациента, обеспечивает доступ пациента к медицинским результатам, документам, удаленную запись на услуги, вызов врача, организацию видеоконференций.
2.1.8. Numedy.Staff – личный кабинет сотрудника, обеспечивает доступ сотрудника Клиента к графикам работы, учебным и информационным материалам.
2.1.9. Numedy.ServiceControl – личный кабинет инженерной компании, обеспечивает доступ к мониторингу и контролю оборудования Клиентов.
2.1.10. Numedy.Insurance – личный кабинет страховой компании.
2.1.11. Numedy.Customer – личный кабинет заказчика.
2.1.12. Numedy.Audit – личный кабинет контролирующего органа.
2.2. Могут предоставляться дополнительные сервисы: телефония, электронная почта, файловое хранилище.
2.3. Провайдером могут предоставляться Клиентам серверные мощности для размещения клиентских программ, при этом их размещение и взаимодействие с системой определяется в соответствии с договором.

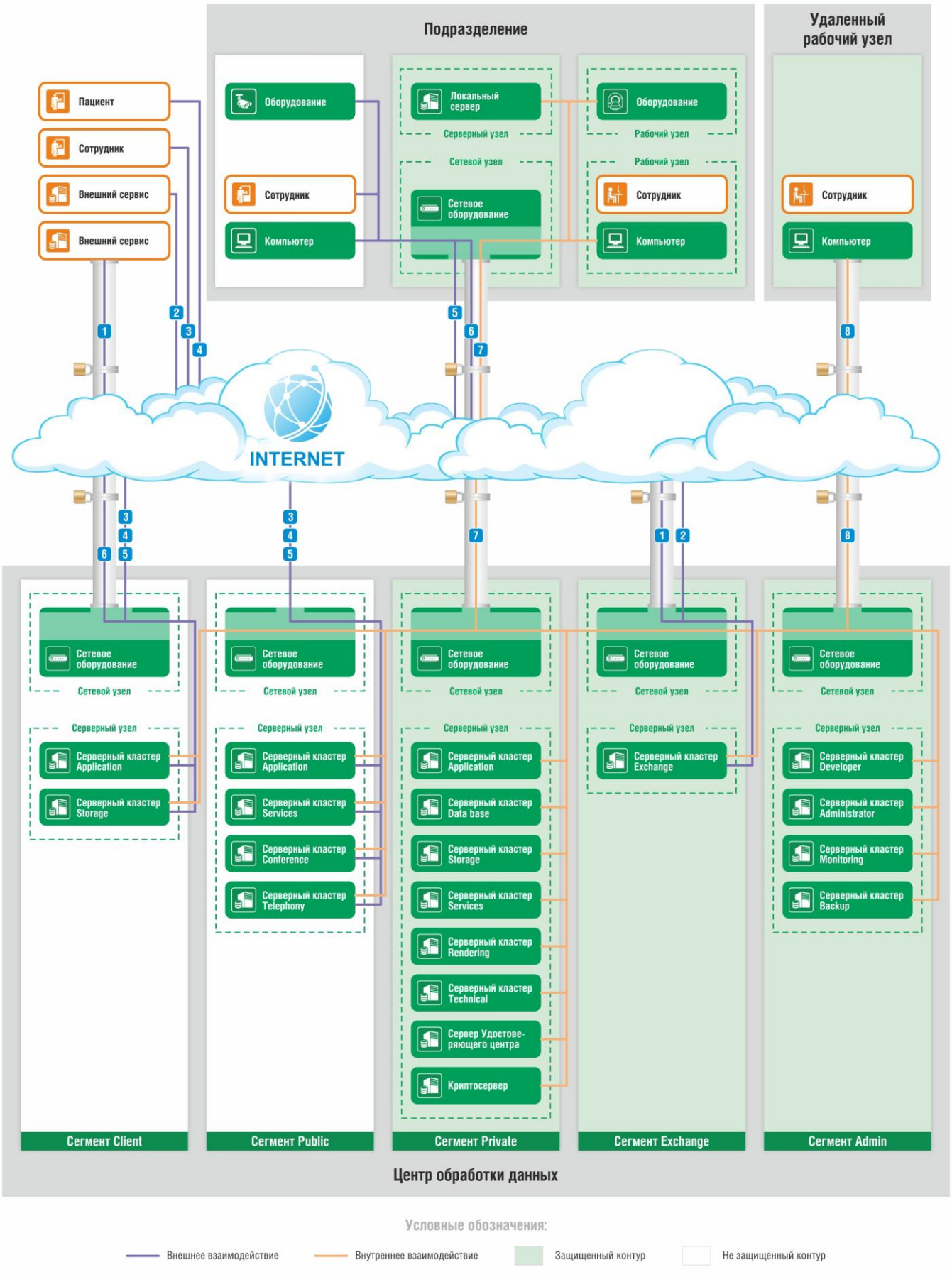
3. Электронная подпись и удостоверяющий центр

3.1. Удостоверяющий центр Провайдера должен быть аккредитован в соответствии с действующим законодательством. Сроки аккредитации удостоверяющего центра должны контролироваться.
3.2. Порядок работы удостоверяющего центра определяется в соответствии с регламентом «Удостоверяющий центр», который формируется в соответствии с требованиями законодательства.
3.3. Электронная подпись, выдаваемая удостоверяющим центром Провайдера, является квалифицированной.
3.4. Оператором удостоверяющего центра является сотрудник Провайдера, занимающий должность Регистратор.
3.5. Работа с электронной подписью разделяется на процессы: создание и выдача электронной подписи, подписание данных электронной подписью и аннулирование (отзыв сертификата) электронной подписи.
3.6. Электронная подпись выдается сотрудникам при получении ими доступов к системе. Срок действия электронной подписи - 3 года. Продление электронной подписи производится до истечения срока действия за один месяц в виде выдачи новой электронной подписи. Аннулирование электронной подписи производится при прекращении доступов сотрудников к системе.
3.7. Электронные подписи хранятся на криптосервере и не передаются пользователям на физических носителях. Криптосервер имеет встроенные средства защиты информации.

4. Состав системы

4.1. Система состоит из сетевых, серверных и рабочих узлов. Узлы объединяются в сегменты по функциональному назначению.
4.2. Оборудование и программное обеспечение, настройки и коммутации сетевых и серверных узлов определяются регламентом «Инфраструктура».
4.3. Оборудование и программное обеспечение, настройки рабочих узлов определяются Проектом подключения и актами подключения к системе.
4.4. Использование иного оборудования и программного обеспечения не допускается.
4.5. Используемое программное обеспечение должно иметь подтверждение его законного использования.
4.6. Состав системы указан на схеме:

Numedy. Состав системы



5. Данные в системе

5.1. В системе обрабатываются следующие данные:

5.1.1. Общие персональные данные пациентов и сотрудников: фамилия, имя, отчество, дата рождения, пол, гражданство, место рождения, адреса, контактная информация, информация о документах, удостоверяющих личность, и страховых полисах, информация о родстве и иные данные.

5.1.2. Биометрические персональные данные сотрудников: отпечатки пальцев.

5.1.3. Персональные данные о состоянии здоровья пациентов: медицинские измерения, протоколы и документы, информация о медицинской помощи, диагнозы, назначения, результаты экспертиз и исследований, медицинские снимки и файлы и другая информация о здоровье пациента.

5.1.4. Данные о хозяйственной деятельности: учетная, справочная, финансовая, кадровая, юридическая и другая хозяйственная информация компаний.

5.1.5. Ключевые данные: логины, пароли, ключи и электронные подписи.

5.1.6. Технические данные: конфигурационные файлы, информация о настройках, техническая документация.

5.1.7. Прочие данные: материалы информационного характера, справочные, учебные и научные данные.

5.2. Обработка персональных данных производится на основании Согласий на обработку информации, полученных от пациентов и сотрудников.

5.3. Оператором персональных данных является Провайдер и Клиент. Данные обрабатываются автоматизировано.

5.4. Политика обработки персональных данных отражается в Политике конфиденциальности, которая публикуется на сайтах Провайдера и Клиентов.

5.5. Уведомление об обработке персональных данных направляется Провайдером в уполномоченный орган по защите прав субъектов персональных данных, в соответствии с действующим законодательством.

5.6. При обращении пациента или сотрудника по вопросам обработки или прекращения обработки персональных данных ответ должен предоставляться в течение не более 15 дней.

6. Доступы в системе

6.1. В системе используются следующие доступы:

6.1.1. Доступ пользователей к инфраструктуре – доступ к оборудованию и программному обеспечению, всем настройкам и коммуникациям сетевых и серверных узлов. Разделяется на типы прав доступа: привилегированный и обычный доступы. Доступы защищены логином и паролем, а также ключами для некоторого оборудования и программного обеспечения.

6.1.2. Доступ пользователей к сервисам системы – доступ к основным и дополнительным сервисам системы. Разделяется на роли и типы прав доступа: администратор, сотрудник, пациент. Роль «Администратор системы» с типом прав доступа «администратор» является привилегированной. Роли с типом прав доступа «сотрудник» назначаются сотрудникам в зависимости от их функциональных обязанностей. Пациенты имеют доступ с типом прав доступа «пациент». Обработка персональных данных производится в зависимости от роли и имеющихся привилегий в основных сервисах системы, при этом роли медицинского персонала обрабатывают персональные данные о здоровье пациентов. Доступы защищены логином (идентификатором) и паролем, а также биометрической защитой в виде отпечатка пальца для некоторых основных сервисов.

6.1.3. Доступ пользователей к рабочим узлам – доступ к оборудованию, операционной системе и прикладным программам на рабочих узлах. Порядок доступа определяется Клиентом.

6.1.4. Доступ оборудования к сервисам системы - доступ оборудования рабочих узлов к сервисам системы. Доступ определяется по идентификатору и IP-адресу, при этом обработка персональных и иных данных производится в соответствии с привилегиями рабочего узла.

6.1.5. Доступ пользователей к клиентским программам – доступ к клиентским программам, размещенным на серверных мощностях системы. Порядок доступа определяется в соответствии с договорами.

6.2. Логины (идентификаторы) и пароли сотрудников создаются и присваиваются уполномоченным лицом при предоставлении доступа, при этом для некоторых основных сервисов системы пароли генерируются автоматически. Логины (идентификаторы) и пароли пациентов создаются (изменяются) и присваиваются автоматически, при этом пациент может самостоятельно изменить пароль.

6.3. Хранение логинов (идентификаторов) в системе производится в явном виде, хранение паролей производится в скрытом, не доступном для прочтения, виде.

6.4. При создании логина (идентификатора) автоматически создается учетная запись.

6.5. В основных сервисах системы реализован механизм сессий, при котором доступ возможен только во время активной сессии. После успешной идентификации, аутентификации и получения доступа, сессии создаются и прекращаются автоматически в зависимости от ролей, привилегий пользователей и оборудования. Исключается повторное использование логина (идентификатора) в течение активной сессии.

6.6. Прекращение доступа производится уполномоченным лицом путем блокировки учетной записи, при этом блокировка может производиться автоматически для некоторых основных сервисов системы.

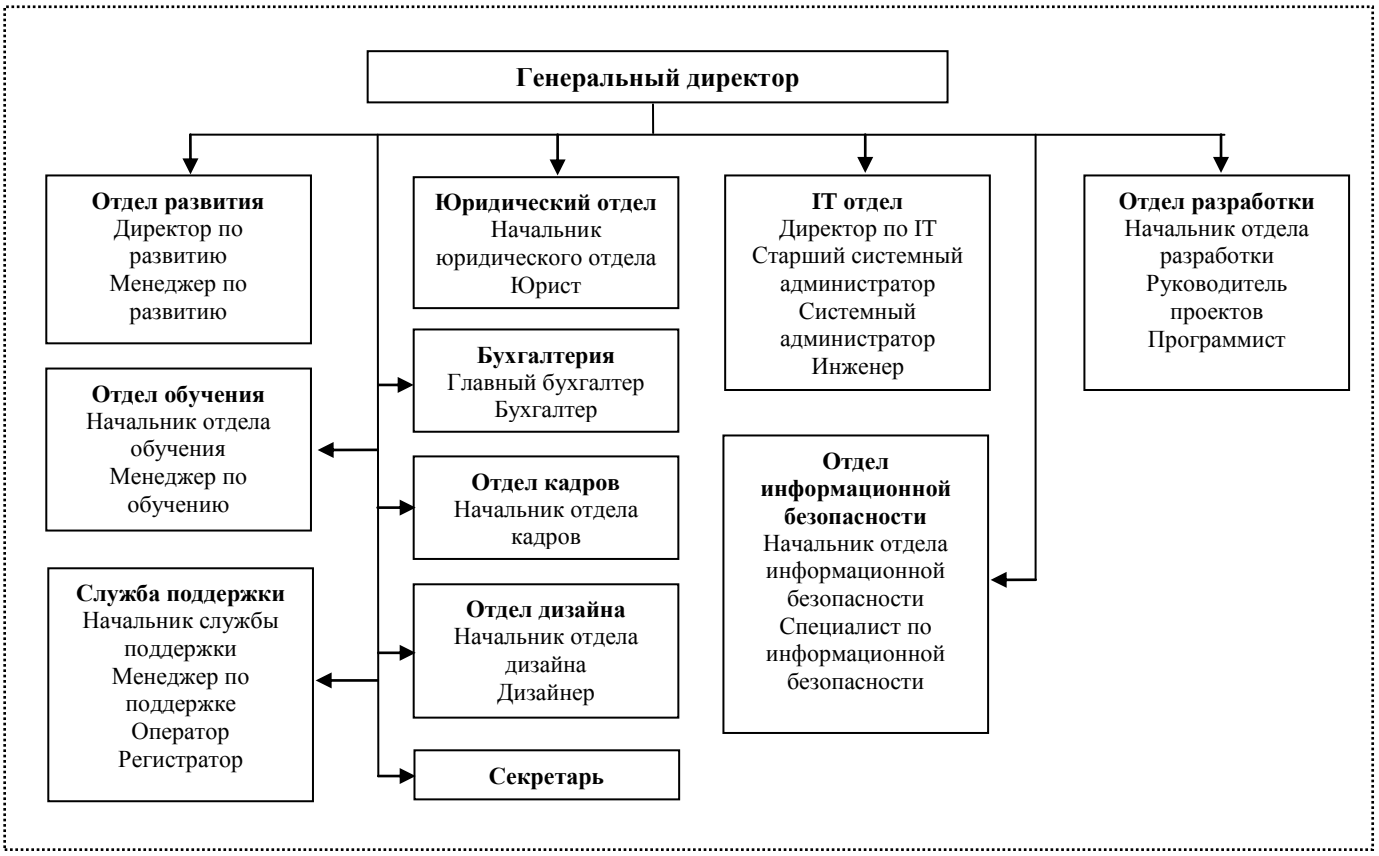
6.7. В сервисе Numedy.AtlasPatient пациенту предоставляется доступ только к собственным персональным данным, доступ к которым пациент имеет право на основании законодательства. При этом обработка персональных данных, кроме доступа (просмотра и извлечения), не производится.

Глава 3. Управление

1. Общие положения

1.1. Провайдер осуществляет лицензируемые виды деятельности и должен иметь лицензии на:
1.1.1. Деятельность по разработке и производству средств защиты конфиденциальной информации.
1.1.2. Деятельность по технической защите конфиденциальной информации.
1.1.3. Деятельность в отношении шифровальных (криптографических) средств.

2. Административная структура Провайдера



3. Подключение к системе

3.1. Подключение Клиента к системе производится на основании договора с Провайдером.
3.2. Подключение Клиента производится в соответствии с Проектом подключения и на основании актов подключения к системе. Изменение подключений узлов к системе производится на основании актов подключения к системе.
3.3. При подключении Клиента к системе производится обучение сотрудников Клиента работе в системе в соответствии с договором.

4. Предоставление и прекращение доступов

4.1. Привилегированный тип доступа к инфраструктуре и роль «Администратор системы» в основных сервисах системы назначается Директору по IT и фиксируется в Журнале доступов.
4.2. Обычный тип доступа к инфраструктуре предоставляется или прекращается Директором по IT по запросам сотрудников Провайдера, сотрудников подрядных компаний и с согласия Генерального директора и фиксируется в Журнале доступов.
4.3. Доступ к сервисам системы предоставляется сотрудникам Регистратором по заявкам при приеме на работу, при этом Регистратором удостоверяется личность, вносятся биометрические данные (отпечатки пальцев) и другая информация (фото, прочие данные) и создается (и выдается) электронная подпись. Роли сотрудников устанавливаются при формировании заявок. Доступ к сервисам системы прекращается автоматически при увольнении сотрудника, при этом аннулируется электронная подпись. Доступ к сервисам системы предоставляется пациентам сотрудниками Клиента (после удостоверения личности) в подразделениях или иным способом, и прекращается Начальником службы поддержки по заявлениям пациентов.
4.4. Доступ к рабочим узлам определяется Клиентом при подключении рабочих узлов к системе, при этом Провайдеру предоставляется привилегированный доступ к операционной системе рабочих узлов.

4.5. Доступ оборудования к сервисам системы предоставляется при подключении рабочих узлов к системе. Доступ прекращается при отключении рабочих узлов от системы.
4.6. Доступ к клиентским программам предоставляется или прекращается Директором по IT или уполномоченным им сотрудником Провайдера в соответствии с договорными отношениями.

5. Обеспечение работы и обслуживание системы

5.1. Работа сетевых и серверных узлов должна быть бесперебойной и круглосуточной. Работа рабочих узлов должна быть бесперебойной и соответствовать режиму работы подразделений и сотрудников.
5.2. Установка и настройка оборудования и программного обеспечения сетевых и серверных узлов должна производиться в соответствии с регламентом «Инфраструктура». Установка и настройка оборудования и программного обеспечения на рабочих узлах должна производиться в соответствии с Проектом подключения и руководствами по установке и настройке. Устанавливаемое программное обеспечение должно пройти антивирусную проверку.
5.3. Мониторинг оборудования и программного обеспечения должен проводиться ежедневно. Инциденты, связанные с работой оборудования и программного обеспечения, фиксируются в Журнале инцидентов.
5.4. Резервное копирование данных производится по расписанию и автоматически. Восстановление данных из резервных копий фиксируется в Журнале инцидентов.
5.5. Техническое обслуживание оборудования производится в соответствии с планами обслуживания.
5.6. Для обслуживания оборудования и программного обеспечения могут привлекаться специализированные организации на основании договоров и с обязательным соглашением о конфиденциальности.
5.7. Начальник отдела информационной безопасности назначается ответственным за информационную безопасность приказом Провайдера.
5.8. При выявлении вредоносных программ (вирусов) средствами антивирусной защиты необходимо провести анализ необходимости использования зараженных вирусом файлов, провести лечение или уничтожение зараженных файлов, в случае обнаружения нового вируса, не поддающегося лечению применяемыми средствами антивирусной защиты, исключить такой файл из обработки.

6. Ответственность сотрудников Провайдера

6.1. Генеральный директор ответственный за:
6.1.1. Контроль предоставления и прекращения доступов к инфраструктуре.
6.2. Директор по IT ответственный за:
6.2.1. Подтверждение законного использования программного обеспечения.
6.2.2. Обеспечение бесперебойной и круглосуточной работы сетевых и серверных узлов системы.
6.2.3. Установку и настройку оборудования и программного обеспечения (и их обновлений) на сетевых и серверных узлах системы.
6.2.4. Мониторинг оборудования и программного обеспечения и немедленное реагирование и принятие мер при инцидентах.
6.2.5. Резервное копирование и восстановление данных из резервных копий.
6.2.6. Организацию предоставления и прекращения доступов к инфраструктуре и клиентским программам.
6.2.7. Организацию технического обслуживания оборудования сетевых и серверных узлов системы.
6.3. Начальник отдела информационной безопасности ответственный за:
6.3.1. Обеспечение информационной безопасности и обработки персональных данных в системе.
6.3.2. Контроль актуальности сертификатов на средства защиты информации.
6.3.3. Установку, настройку, обслуживание и учет средств защиты информации.
6.3.4. Оценку эффективности и контроль принимаемых мер по обеспечению безопасности.
6.3.5. Управление средствами антивирусной защиты и обнаружения вторжений и обновление базы данных признаков вредоносных компьютерных программ (вирусов) и базы решающих правил.
6.3.6. Аттестацию сегментов системы по требованиям к государственным информационным системам.
6.3.7. Тестирование системы на проникновения.
6.3.8. Мониторинг информационной безопасности и немедленное реагирование и принятие мер при инцидентах.
6.4. Директор по развитию ответственный за:
6.4.1. Подготовку подключения Клиента к системе и формирование Проекта подключения.
6.5. Начальник службы поддержки ответственный за:
6.5.1. Организацию и контроль предоставления и прекращения пользовательских доступов к системе.
6.5.2. Организацию и контроль выдачи, продления и аннулирования электронных подписей.
6.5.3. Организацию подключения к системе и контроль изменений подключения к системе.
6.5.4. Работу с обращениями пациентов и сотрудников.
6.5.5. Контроль предоставления и прекращения доступов к сервисам системы.
6.6. Начальник отдела обучения ответственный за:
6.6.1. Обучение сотрудников работе в системе.
6.7. Начальник юридического отдела ответственный за:
6.7.1. Ведение договорных отношений Провайдера.
6.7.2. Регистрацию системы как медицинского изделия и контроль условий регистрационного удостоверения.
6.7.3. Регистрацию системы как программы ЭВМ и регистрацию необходимых изменений.

6.7.4. Получение лицензий на лицензируемые виды деятельности и контроль выполнения лицензионных требований.
6.7.5. Направление уведомления об обработке персональных данных и своевременное внесение изменений.
6.7.6. Аккредитацию удостоверяющего центра и контроль сроков аккредитации.

7. Ответственность Клиента

7.1. Клиент в соответствии с договором с Провайдером и в лице уполномоченных сотрудников обязан:
7.1.1. Назначить ответственных сотрудников Клиента за поддержание инфраструктуры и за информационную безопасность.
7.1.2. Разместить на сайте Клиента предоставленную Провайдером Политику конфиденциальности.
7.1.3. Получать у пациента Согласия на обработку информации и организовать хранение полученных Согласий на обработку информации.
7.1.4. Обеспечить размещение сетевых и серверных узлов подразделений в коммуникационных шкафах, оборудованных кодовыми замками (или системой биометрического доступа) и обеспечить допуск к ним только уполномоченных лиц. При необходимости и в соответствии с проектом подключения, оборудовать помещения, где установлены коммуникационные шкафы, системами видеонаблюдения и охранной сигнализации.
7.1.5. Предоставить Провайдеру привилегированный доступ к операционным системам рабочих узлов.
7.2. Сотрудник Клиента, ответственный за поддержание инфраструктуры, должен обеспечивать:
7.2.1. Бесперебойную работу рабочих узлов Клиента.
7.2.2. Установку и настройку оборудования и программного обеспечения рабочих узлов Клиента.
7.2.3. Взаимодействие с сотрудниками Провайдера по установке, настройке и работе оборудования и программного обеспечения.
7.2.4. Немедленное реагирование на инциденты, связанные с работой оборудования и программного обеспечения.
7.2.5. Техническое обслуживание оборудования рабочих узлов Клиента.
7.3. Сотрудник Клиента, ответственный за информационную безопасность, должен обеспечивать:
7.3.1. Взаимодействие с сотрудниками Провайдера по работе средств защиты.
7.3.2. Немедленное реагирование на инциденты, связанные с информационной безопасностью.
7.4. Сотрудникам Клиента не допускается передавать другим лицам данные для доступа в систему.

Глава 4. Информационная безопасность

1. Общие положения

1.1. Система является распределенной, сегментированной, многопользовательской, некоторые ее сегменты имеют централизованное подключение к сетям общего пользования, в том числе к информационно-телекоммуникационным сетям.
1.2. Защите подлежат следующие объекты:
1.2.1. Персональные данные, данные о хозяйственной деятельности и ключевые данные.
1.2.2. Информационные каналы.
1.2.3. Оборудование и программное обеспечение сегментов системы, в которых обрабатываются данные, подлежащие защите.
1.3. Контролируемой зоной являются: центр обработки данных и подразделения.
1.4. Медицинское оборудование, устанавливаемое на рабочих узлах и имеющее регистрационное удостоверение, формирует (создает) персональные данные о состоянии здоровья пациентов, что не является обработкой персональных данных.
1.5. Сохранение на рабочих узлах каких-либо файлов, содержащих защищаемые данные, не предусмотрено.

2. Классификация

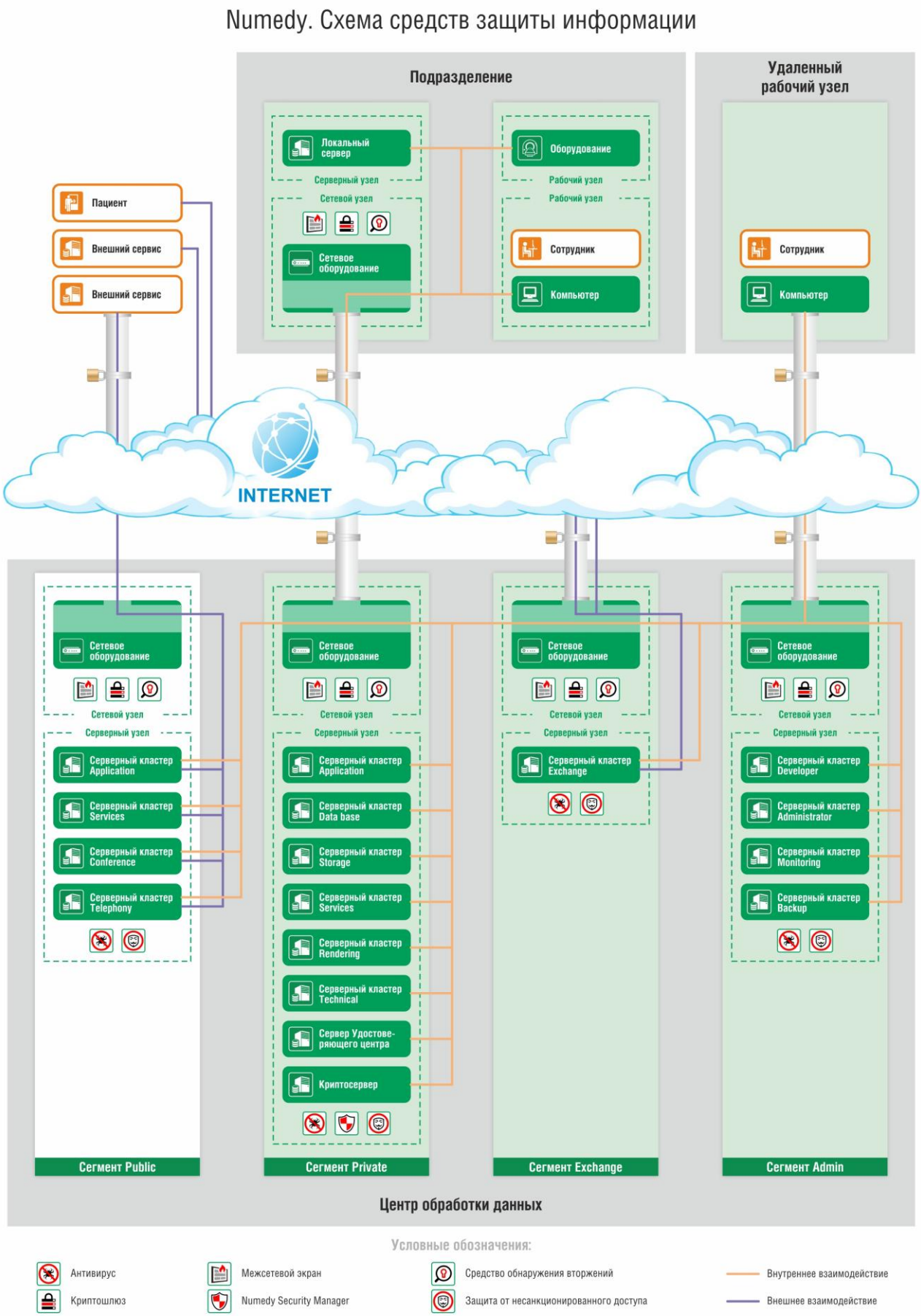
2.1. Для системы устанавливается необходимость обеспечения 2-го уровня защищенности персональных данных в соответствии с требованиями законодательства. На основании того, что для системы актуальны угрозы 3-го типа и система обрабатывает специальные категории персональных данных (данные о состоянии здоровья) более чем 100 000 субъектов персональных данных, не являющихся сотрудниками, и биометрические данные.
2.2. Для обеспечении 2-го уровня защищенности персональных данных в соответствии с требованиями действующего законодательства может применяться уровень криптозащиты КС1.
2.3. Для обеспечения 2-го уровня защищенности персональных данных в соответствии с требованиями действующего законодательства должны применяться средства защиты:
2.3.1. Не ниже 4 класса для системы обнаружения вторжений и средств антивирусной защиты.
2.3.2. Не ниже 4 класса для межсетевых экранов.
2.3.3. Программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

3. Специальные требования и условия

3.1. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных должна проводиться до ввода системы в эксплуатацию.
3.2. Первичный контроль принимаемых мер по обеспечению безопасности персональных данных должен проводиться при вводе информационной системы в эксплуатацию.
3.3. Периодический контроль принимаемых мер по обеспечению безопасности персональных данных должен проводиться два раза в год в апреле и ноябре.
3.4. Тестирование системы на проникновения должно проводиться ежемесячно.
3.5. Мониторинг информационной безопасности должен проводиться постоянно. Инциденты, связанные с информационной безопасностью, фиксируются в Журнале инцидентов.
3.6. Сегмент системы Exchange government подлежит аттестации по требованиям к государственным информационным системам, как информационная система персональных данных «Numedy Exchange».
3.7. Управление средствами антивирусной защиты и обнаружения вторжений должно быть централизованными. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) и базы решающих правил должно проводиться периодически.

4. Средства защиты информации

4.1. Используемые в системе средства защиты информации должны иметь необходимые действующие сертификаты, выданные уполномоченными органами.
4.2. Все используемые или хранящиеся средства защиты, а так же документация на них, подлежат учету. Учетная информация отражается в Журнале учета средств защиты.
4.3. Установка и обслуживание средств защиты может производиться подрядчиком, имеющим необходимые лицензии, в соответствии с договором и с обязательным соглашением о конфиденциальности.
4.4. В системе используются средства защиты информации, в том числе средства криптографической защиты каналов передачи информации, в соответствии со схемой:



В качестве средства защиты «Антивирус» может применяться Kaspersky.Endpoint Security, в качестве средств защиты «Криптошлюз» и «Межсетевой экран» могут применяться VipNet Coordinator или Diamond VPN/FW или VipNet Client или Diamond Client, в качестве средства защиты «Средство обнаружения вторжений» могут применяться Diamond VPN/FW или VipNet IDS HS, в качестве средства защиты «Защита от несанкционированного доступа» может применяться DallasLock.

5. Определение угроз безопасности персональных данных

5.1. В системе может быть возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны, т.к. реализован комплекс организационных и технических мер защиты персональных данных.

5.2. Анализ актуальности базовых угроз безопасности персональных данных в системе:

5.2.1. Угрозы утечки информации по техническим каналам. Угрозы неактуальны, т.к. отсутствует функционал ввода или воспроизведения акустической информации, утечки видовой информации исключены организационными мерами, а утечки за счет электромагнитных излучений технически затруднены.

5.2.2. Угрозы несанкционированного доступа к персональным данным, обрабатываемым на рабочих узлах. Угрозы неактуальны, т.к. в системе реализована защита от несанкционированного доступа.

5.2.3. Угрозы несанкционированного доступа к персональным данным со стороны вредоносных программ и угрозы внедрения вредоносных программ. Угрозы неактуальны, т.к. в системе реализованы антивирусная защита и система обнаружения вторжений.

5.2.4. Угрозы несанкционированного доступа к персональным данным с использованием аппаратных закладок. Угрозы неактуальны, т.к. в системе используется программное обеспечение прошедшее проверку на отсутствие недокументированных возможностей.

5.2.5. Угрозы, возникающие в ходе загрузки операционных систем. Угрозы неактуальны, т.к. в системе доступ к серверам производится с помощью браузера и операционная система на рабочих узлах не влияет на безопасность доступов к серверам.

5.2.6. Угрозы, возникающие после загрузки операционных систем. Угрозы неактуальны, т.к. в системе доступ к серверам производится с помощью браузера и операционная система на рабочих узлах не влияет на безопасность доступов к серверам.

5.2.7. Угрозы из внешних сетей. Угрозы неактуальны, т.к. применяется криптозащита информационных каналов, а доступ к сетям общего пользования производится централизованно с применением межсетевого экранирования.

5.3. Для системы неактуальны базовые угрозы безопасности персональных данных, соответственно информационная система имеет высокую степень защищенности.

5.4. Для системы теоретически могут быть актуальны только некоторые угрозы безопасности, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении (угрозы 3 типа).

6. Оценка вреда, который может быть причинен субъектам персональных данных

6.1. В случае реализации угроз нарушения конфиденциальности, целостности и доступности персональных данных может быть причинен моральный и материальный вред пациентам и сотрудникам и нанесен репутационный и материальный ущерб Провайдеру и Клиенту.

6.2. Оценка вреда, который может быть причинен пациентам:

Угроза безопасности	Оценка морального вреда	Оценка материального вреда
Распространение общих персональных данных пациента	средний	размер компенсации морального вреда
Несанкционированный доступ к общим персональным данным пациента	минимальный	
Неправомерное изменение общих персональных данных пациента	минимальный	
Блокирование доступа к общим персональным данным пациента	минимальный	
Уничтожение общих персональных данных пациента	минимальный	
Распространение данных о состоянии здоровья пациента	максимальный	
Несанкционированный доступ к данным о состоянии здоровья пациента	средний	
Неправомерное изменение данных о состоянии здоровья пациента	максимальный	размер компенсации морального вреда и затраты на устранение последствий возможной врачебной ошибки
Блокирование доступа к данным о состоянии здоровья пациента	минимальный	
Уничтожение данных о состоянии здоровья пациента	средний	

Размер компенсации морального вреда на основании анализа судебных решений может составить порядка 25 000 рублей для общих персональных данных и 50 000 рублей для данных о состоянии здоровья.
Затраты на устранение последствий возможной врачебной ошибки зависят от последствий в каждом конкретном случае.

6.3. Оценка вреда, который может быть причинен сотрудникам:

Угроза безопасности	Оценка морального вреда	Оценка материального вреда
Распространение общих персональных данных сотрудника	средний	размер компенсации морального вреда
Несанкционированный доступ к общим персональным данным сотрудника	минимальный	
Неправомерное изменение общих персональных данных сотрудника	минимальный	
Несанкционированный доступ к биометрическим данным сотрудника	средний	устранение последствий несанкционированного доступа
Неправомерное изменение биометрических данных сотрудника	максимальный	

Размер компенсации морального вреда на основании анализа судебных решений может составить порядка 15 000 рублей. Последствия несанкционированного доступа в МИС определяются для каждого случая.

6.4. Соотношение принимаемых мер по защите персональных данных и возможного ущерба при причинении вреда пациентам и сотрудникам в случае реализации угроз безопасности:

Меры по защите персональных данных	Возможный репутационный ущерб	Возможный материальный ущерб
Обеспечение конфиденциальности общих персональных данных пациента	большой	средний
Обеспечение целостности общих персональных данных пациента	средний	средний
Обеспечение доступности общих персональных данных пациента	средний	средний
Обеспечение конфиденциальности данных о состоянии здоровья пациента	очень большой	большой
Обеспечение целостности данных о состоянии здоровья пациента	большой	большой
Обеспечение доступности данных о состоянии здоровья пациента	большой	большой
Обеспечение конфиденциальности общих персональных данных сотрудника	незначительный	незначительный
Обеспечение целостности общих персональных данных сотрудника	незначительный	незначительный
Обеспечение доступности общих персональных данных сотрудника	незначительный	незначительный
Обеспечение конфиденциальности биометрических данных сотрудника	незначительный	большой
Обеспечение целостности биометрических данных сотрудника	незначительный	большой

Размер возможного материального ущерба определяется: размерами компенсаций морального вреда пациентам и сотрудникам, размерами компенсаций затрат пациентам на устранение последствий возможных врачебных ошибок, штрафами за нарушение законодательства, затратами на проведение технических мероприятий по устранению последствий инцидентов, затратами на проведение контроля эффективности системы защиты, затратами на устранение последствий репутационного ущерба.

6.5. Для Провайдера и Клиента существуют риски нанесения репутационного и материального ущерба, связанные с реализацией угроз безопасности персональных данных. В связи с этим целесообразно реализовывать максимально усиленные меры по защите персональных данных.

7. Меры по защите персональных данных

7.1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

7.1.1. ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора. Требования ИАФ.1 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.1.2. ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных. мобильных и портативных. Требования ИАФ.2 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.1.3. ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. Требования ИАФ.3 обеспечиваются с помощью средства защиты Numedy.SecurityManager и регулируются настоящим регламентом.

7.1.4. ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Требования ИАФ.4 обеспечиваются с помощью средства защиты Numedy.SecurityManager и регулируются настоящим регламентом.

7.1.5. ИАФ.5 Защита обратной связи при вводе аутентификационной информации. Требования ИАФ.5 обеспечиваются с помощью средства защиты Numedy. SecurityManager.

7.1.6. ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей). Требования ИАФ.6 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.2. Управление доступом субъектов доступа к объектам доступа (УПД).

7.2.1. УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. Требования УПД.1 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.2.2. УПД.2 Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) разграничения доступа. Требования УПД.2 обеспечиваются с помощью средства защиты Numedy.SecurityManager и регулируются настоящим регламентом.

7.2.3. УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а так же между информационными системами. Требования УПД.3 обеспечиваются с помощью средства защиты (межсетевой экран) VipNet.Coordinator или Diamond VPN/FW и регулируется регламентом «Инфраструктура».

7.2.4. УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы. Требования УПД.4 обеспечиваются с помощью средства защиты Numedy.SecurityManager и регулируются настоящим регламентом.

7.2.5. УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. Требования УПД.5 обеспечиваются и регулируются настоящим регламентом.

7.2.6. УПД.6 Ограничение неуспешных попыток входа в информационную систему. В системе не производится ограничение неуспешных попыток входа, т.к. угроза безопасности не является актуальной, а так же в системе применяется защита от несанкционированного доступа.

7.2.7. УПД.7 Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных. Требования УПД.7 для системы не установлены, но в сервисе Numedy.AtlasPatient используется предупреждение о реализации мер по обеспечению безопасности персональных данных.

7.2.8. УПД.8 Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему. Требования УПД.8 для системы не установлены и не применяются.

7.2.9. УПД.9 Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы. Требования УПД.9 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.2.10. УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя или по его запросу. Требования УПД.10 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.2.11. УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации. В системе не предусмотрен доступ без идентификации и аутентификации.

7.2.12. УПД.12 Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки. Требования УПД.12 для системы не установлены и не применяются.

7.2.13. УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети. В системе доступ к объектам доступа через внешние информационно-телекоммуникационным сети не предусмотрен.

7.2.14. УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа. В системе в контролируемой зоне не используются технологии беспроводного доступа. Технологии беспроводного доступа для удаленных рабочих узлов используются с применением средств защиты VipNet. Client.

7.2.15. УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств. В системе не используются мобильные технические средства.

7.2.16. УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы). Требования УПД.16 обеспечиваются взаимодействием с внешними сервисами (информационными системами) с помощью аттестованного сегмента системы и сервиса Numedy. Exchange.

7.2.17. УПД.17 Обеспечение доверенной загрузки средств вычислительной техники. В системе требования УПД.17 неактуальны, кроме сегмента Numedy. Exchange government, в котором используется сертифицированное средство защиты информации - средство доверенной загрузки DallasLock.

7.3. Ограничение программной среды (ОПС).

7.3.1. ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения. Требования ОПС.1 для системы не установлены и не применяются.

7.3.2. ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой программного обеспечения. Требования ОПС.2 обеспечиваются и регулируются настоящим регламентом.

7.3.3. ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов. Требования ОПС.3 для системы не установлены, но обеспечиваются и регулируются настоящим регламентом.

7.3.4. ОПС.4 Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов. Требования ОПС.4 для системы не установлены и не применяются.

7.4. Защита машинных носителей информации (ЗНИ).

7.4.1. ЗНИ.1 Учет машинных носителей информации. В системе учет машинных носителей информации не требуется, т.к. не производится запись\хранение защищаемых данных на машинных носителях на рабочих узлах и не используются съемные машинные носители. Для записи защищаемых данных используются только накопители, расположенные в защищаемом сегменте серверного узла, при этом при извлечении машинного накопителя чтение данных невозможно.

7.4.2. ЗНИ.2 Управление доступом к машинным носителям информации. В системе управление доступом к машинным носителям информации не требуется, т.к. не производится запись\хранение защищаемых данных на машинных носителях на рабочих узлах и не используются съемные машинные носители. Для записи защищаемых данных используются только накопители, расположенные в защищаемом сегменте серверного узла, при этом при извлечении машинного накопителя чтение данных не возможно.

7.4.3. ЗНИ.3 Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны. Требования ЗНИ.3 для системы не установлены и не применяются.

7.4.4. ЗНИ.4 Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах. Требования ЗНИ.4 для системы не установлены и не применяются.

7.4.5. ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных. Требования ЗНИ.5 для системы не установлены и не применяются.

7.4.6. ЗНИ.6 Контроль ввода (вывода) информации на машинные носители персональных данных. Требования ЗНИ.6 для системы не установлены и не применяются.

7.4.7. ЗНИ.7 Контроль подключения машинных носителей персональных данных. Требования ЗНИ.7 для системы не установлены и не применяются.

7.4.8. ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а так же контроль уничтожения (стирания). В системе уничтожение информации на машинных носителях не требуется, т.к. не производится передача машинных носителей, а при извлечении носителя чтение данных не возможно.

7.5. Регистрация событий безопасности (РСБ).

7.5.1. РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения. Требования РСБ.1 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.5.2. РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации. Требования РСБ.2 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.5.3. РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения. Требования РСБ.3 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.5.4. РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема памяти. Требования РСБ.4 для системы не установлены и не применяются.

7.5.5. РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Требования РСБ.5 обеспечиваются с помощью средства защиты Numedy.SecurityManager и регулируются настоящим регламентом.

7.5.6. РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в информационной системе. Требования РСБ.6 для системы не установлены и не применяются.

7.5.7. РСБ.7 Защита информации о событиях безопасности. Требования РСБ.7 обеспечиваются с помощью средства защиты Numedy.SecurityManager.

7.6. Антивирусная защита (АВЗ).

7.6.1. АВЗ.1 Реализация антивирусной защиты. Требования АВЗ.1 обеспечиваются с помощью средства защиты Kaspersky. Endpoint Security и регулируются настоящим регламентом.

7.6.2. АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). Требования АВЗ.2 обеспечиваются и регулируются настоящим регламентом.

7.7. Обнаружение вторжений (СОВ).

7.7.1. СОВ.1 Обнаружение вторжений. Требования СОВ.1 обеспечиваются с помощью средств защиты Diamond VPN/FW или VipNet IDS HS и регулируется настоящим регламентом.

7.7.2. СОВ.2 Обновление базы решающих правил. Требования СОВ.2 обеспечиваются и регулируются настоящим регламентом.

7.8. Контроль (анализ) защищенности информации (АНЗ).

7.8.1. АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. Требования АНЗ.1 обеспечиваются и регулируются настоящим регламентом.

7.8.2. АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Требования АНЗ.2 обеспечиваются и регулируются настоящим регламентом.

7.8.3. АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. Требования АНЗ.3 обеспечиваются и регулируются настоящим регламентом.

7.8.4. АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации. Требования АНЗ.4 обеспечиваются Начальником отдела информационной безопасности.

7.8.5. АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе. Требования АНЗ.5 обеспечиваются Начальником отдела информационной безопасности.

7.9. Обеспечение целостности информационной системы и информации (ОЦЛ).

7.9.1. ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. Требования ОЦЛ.1 обеспечиваются с помощью средства защиты Numedy. SecurityManager.

7.9.2. ОЦЛ.2 Контроль целостности персональных данных, содержащихся в базах данных информационной системы. Требования ОЦЛ.2 для системы не установлены и не применяются.

7.9.3. ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций. Требования ОЦЛ.3 для системы не установлены и не применяются.

7.9.4. ОЦЛ.4 Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама). Требования ОЦЛ.4 для системы неактуальны.

7.9.5. ОЦЛ.5 Контроль содержания информации, передаваемой из информационной системы и исключение неправомерной передачи информации из информационной системы. Требования ОЦЛ.5 для системы не установлены и не применяются.

7.9.6. ОЦЛ.6 Ограничение прав пользователей по вводу информации в информационную систему. Требования ОЦЛ.6 для системы не установлены и не применяются.

7.9.7. ОЦЛ.7 Контроль точности, полноты и правильности данных, вводимых в информационную систему. Требования ОЦЛ.7 для системы не установлены и не применяются.

7.9.8. ОЦЛ.8 Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях. Требования ОЦЛ.8 для системы не установлены и не применяются.

7.10. Обеспечение доступности информации (ОДТ).

7.10.1. ОДТ.1 Использование отказоустойчивых технических средств. Требования ОДТ.1 для системы не установлены и не применяются.

7.10.2. ОДТ.2 Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы. Требования ОДТ.2 для системы не установлены и не применяются.

7.10.3. ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование. Требования ОДТ.3 для системы не установлены и не применяются.

7.10.4. ОДТ.4 Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных. Требования ОДТ.4 обеспечиваются и регулируются настоящим регламентом.

7.10.5. ОДТ.5 Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала. Требования ОДТ.5 обеспечиваются и регулируются настоящим регламентом.

7.11. Защита среды виртуализации (ЗСВ).

7.11.1. ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.1 для системы неактуальны.

7.11.2. ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.2 для системы неактуальны.

7.11.3. ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.3 для системы неактуальны.

7.11.4. ЗСВ.4 Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры. Требования ЗСВ.4 для системы не установлены и не применяются.

7.11.5. ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией. Требования ЗСВ.5 для системы не установлены и не применяются.

7.11.6. ЗСВ.6 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.6 для системы неактуальны.

7.11.7. ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.7 для системы неактуальны.

7.11.8. ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.8 для системы неактуальны.

7.11.9. ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.9 для системы неактуальны.

7.11.10. ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей. Виртуальная инфраструктура в системе не применяется и требования ЗСВ.10 для системы неактуальны.

7.12. Защита технических средств (ЗТС).

7.12.1. ЗТС.1 Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам. Требования ЗТС.1 для системы не установлены и не применяются.

7.12.2. ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. Требования ЗТС.2 для системы не установлены и не применяются.

7.12.3. ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружениях, в которых они установлены. Требования ЗТС.3 обеспечиваются следующими мерами:

- Для сетевых и серверных узлов, расположенных в центре обработки данных, контроль и управление физическим доступом осуществляется в соответствии с договором с подрядчиком, предоставляющим центр обработки данных.
- Для сетевых и серверных узлов, расположенных в подразделениях, контроль и управление физическим доступом осуществляется Клиентом в соответствии и договором и регулируется настоящим регламентом. Для управления физическим доступом применяются кодовые замки на коммуникационных шкафах, а так же биометрические системы доступа.

7.12.4. ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Требования ЗТС.4 обеспечиваются при формировании проекта подключения следующими мерами: устанавливаются жалюзи на окнах помещений, в которых находятся мониторы и принтеры, исключается несанкционируемый доступ третьих лиц в помещения с помощью кодовых замков, мониторы и принтеры устанавливаются на расстоянии более двух метров от дверей и мест нахождения третьих лиц, мониторы устанавливаются обратной стороной к месту нахождения третьих лиц. Так же с помощью электронной очереди исключается нахождение третьих лиц в метах обслуживания пациентов.

7.12.5. ЗТС.5 Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов). Требования ЗТС.5 обеспечиваются размещением оборудования в пределах контролируемой зоны и обеспечения в ней норм микроклимата, пожарной безопасности, эксплуатации электроустановок, электропитания и заземления оборудования, а так же обеспечение резервного электропитания.

7.13. Защита информационной системы, ее средств и систем связи и передачи данных (ЗИС).

7.13.1. ЗИС.1 Разделение в информационной системе функций по управлению информационной системой, управлению системой защиты информации, функций по обработке информации и иных функций информационной системы. Требования ЗИС.1 для системы не установлены, но обеспечиваются и регулируются настоящим регламентом.

7.13.2. ЗИС.2 Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом. Требования ЗИС.2 для системы не установлены и не применяются.

7.13.3. ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Требования обеспечиваются с помощью средства криптозащиты каналов связи VipNet. Coordinator или Diamond VPN/FW. Для сервиса Numedy. AtlasPatient по требованиям криптозащита каналов связи не требуется, т.к. пациентом производится извлечение собственных персональных данных из защищенного контура.

7.13.4. ЗИС.4 Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации. Требования ЗИС.4 для системы не установлены и не применяются.

7.13.5. ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств. Требования ЗИС.5 для системы не установлены, но обеспечиваются централизованным управлением устройствами с помощью сервиса Numedy.DeviceManager, неактуальные устройства отключаются и блокируются при подключении рабочих узлов к системе.

7.13.6. ЗИС.6 Передача и контроль целостности атрибутов безопасности, связанных с информацией, при обмене информацией с иными информационными системами. Требования ЗИС.6 для системы не установлены и не применяются.

7.13.7. ЗИС.7 Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода. Требования ЗИС.7 для системы не установлены и неактуальны.

7.13.8. ЗИС.8 Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. Требования ЗИС.8 для системы не установлены, но обеспечиваются централизованным управлением устройствами передачи речи с помощью сервиса Numedy.Conference.

7.13.9. ЗИС.9 Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации. Требования ЗИС.9 для системы не установлены, но обеспечиваются централизованным управлением устройствами передачи видеоинформации с помощью сервиса Numedy.Conference.

7.13.10. ЗИС.10 Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам. Требования ЗИС.10 для системы не установлены и не применяются.

7.13.11. ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. Требования ЗИС.11 обеспечивается с помощью механизма сессий в системе.

7.13.12. ЗИС.12 Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю. Требования ЗИС.12 для системы не установлены и неактуальны, т.к. передача персональных данных между пользователями не используется.

7.13.13. ЗИС.13 Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя. Требования ЗИС.13 для системы не установлены и неактуальны, т.к. передача персональных данных между пользователями не используется.

7.13.14. ЗИС.14 Использование устройств терминального доступа для обработки информации. Требования ЗИС.14 для информационной системы не установлены.

7.13.15. ЗИС.15 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных. Требования ЗИС.15 обеспечиваются в системе, т.к. указанная информация входит в объекты защиты и обеспечивается их защита вместе с персональными данными.

7.13.16. ЗИС.16 Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов. Требования ЗИС.16 для системы не установлены и не применяются.

7.13.17. ЗИС.17 Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы. Требования ЗИС.17 обеспечиваются в системе с помощью разделения на сегменты и реализации защиты тех сегментов, в которых обрабатываются данные, подлежащие защите.

7.13.18. ЗИС.18 Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения. Требования ЗИС.18 для системы не установлены и не применяются.

7.13.19. ЗИС.19 Изоляция процессов в выделенной области памяти. Требования ЗИС.19 для системы не установлены и не применяются.

7.13.20. ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе. В системе в контролируемой зоне не используются технологии беспроводного доступа. Технологии беспроводного доступа для удаленных рабочих узлов используются с применением средств защиты VipNet. Client или Diamond Client.

7.14. Выявление инцидентов и реагирование на них (ИНЦ).

7.14.1. ИНЦ.1 Определение лиц, ответственных за выявление инцидентов и реагирование на них. Требования ИНЦ.1 обеспечиваются и регулируются настоящим регламентом.

7.14.2. ИНЦ.2 Обнаружение, идентификация и регистрация инцидентов. Требования ИНЦ.2 обеспечиваются и регулируются настоящим регламентом.

7.14.3. ИНЦ.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами. Требования ИНЦ.3 обеспечиваются и регулируются настоящим регламентом.

7.14.4. ИНЦ.4 Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий. Требования ИНЦ.4 обеспечиваются Начальником отдела информационной безопасности.

7.14.5. ИНЦ.5 Принятие мер по устранению последствий инцидентов. Требования ИНЦ.5 обеспечиваются и регулируются настоящим регламентом.

7.14.6. ИНЦ.6 Планирование и принятие мер по предотвращению повторного возникновения инцидентов. Требования ИНЦ.6 обеспечиваются Начальником отдела информационной безопасности.

7.15. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

7.15.1. УКФ.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных. Требования УКФ.1 обеспечиваются и регулируются настоящим регламентом и регламентом «Инфраструктура».

7.15.2. УКФ.2 Управление изменениями конфигурации информационной системы и системы защиты персональных данных. Требования УКФ.2 обеспечиваются и регулируются настоящим регламентом и регламентом «Инфраструктура».

7.15.3. УКФ.3 Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных. Требования УКФ.3 обеспечиваются Начальником отдела информационной безопасности.

7.15.4. УКФ.4 Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных. Требования УКФ.4 обеспечиваются и регулируются настоящим регламентом и регламентом «Инфраструктура».